

FIG.1

NETWORK ATTACK PROTECTION SYSTEM

100

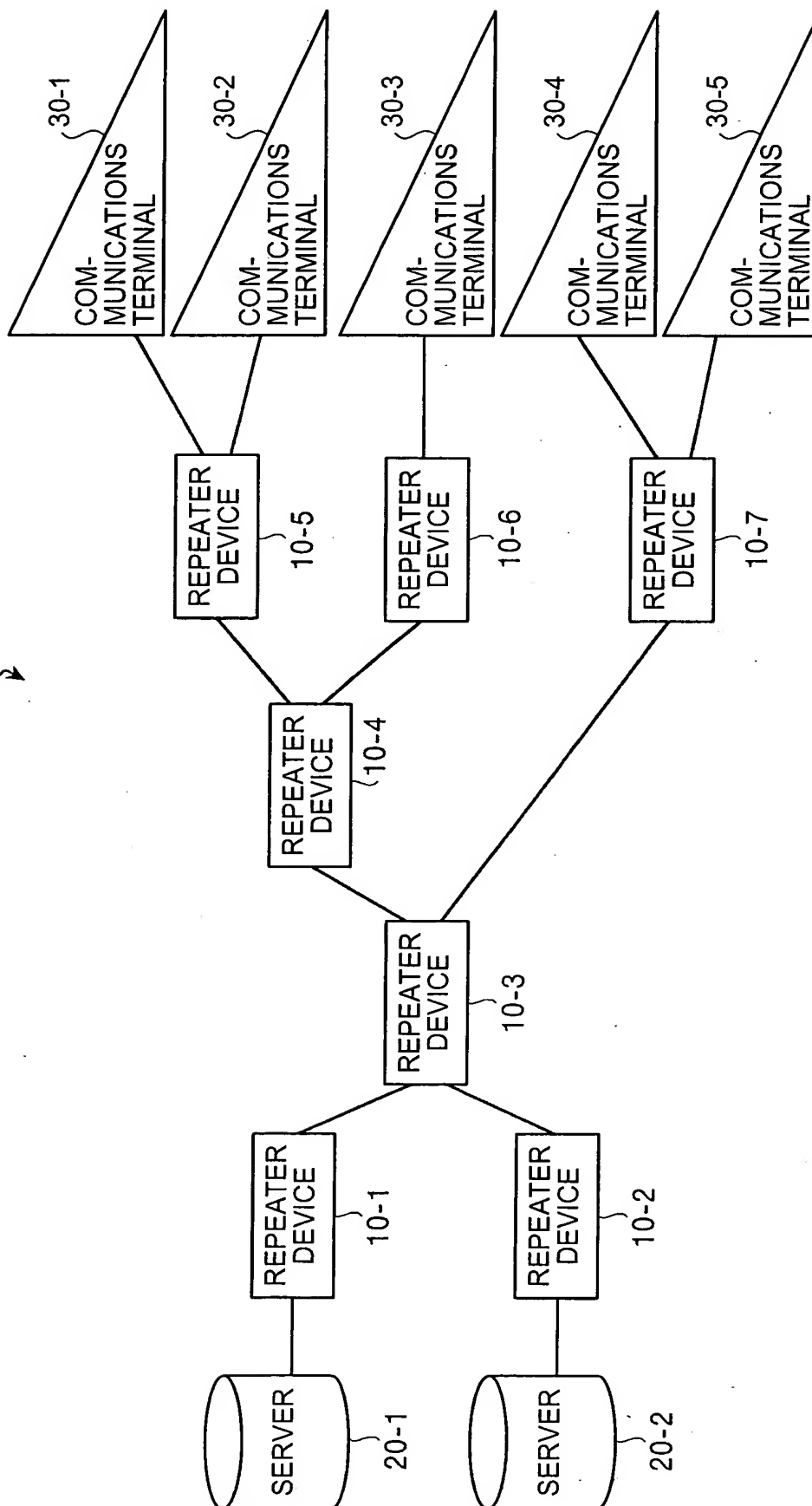
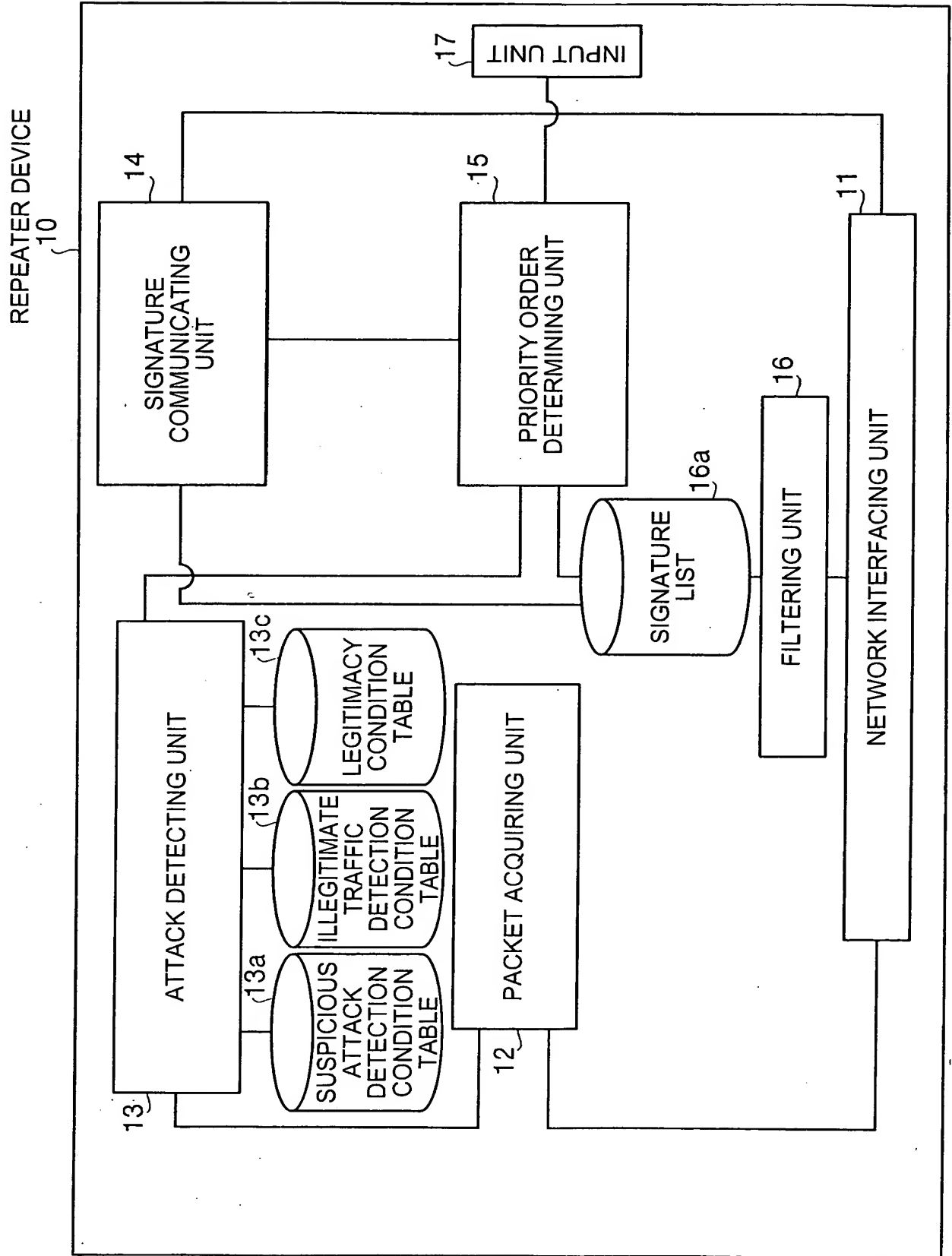


FIG.2



## FIG.3

SUSPICIOUS ATTACK DETECTION CONDITION TABLE

13a

NO.	DETECTION ATTRIBUTES	DETECTION THRESHOLD	DETECTION TIME
1	{Dst=192.168.1.1/32,Protocol=TCP,Port=80}	500 Kbps	10 SECONDS
2	{Dst=192.168.1.2/32,Protocol=UDP}	300 Kbps	10 SECONDS
3	{Dst=192.168.1.1/24}	1000 Kbps	20 SECONDS
⋮			

## FIG.4

ILLEGITIMATE TRAFFIC DETECTION CONDITION TABLE

13b

NO.	ILLEGITIMATE TRAFFIC CONDITIONS
1	PACKETS AT OR MORE ARE CONTINUOUSLY TRANSMITTED FOR S1 SECONDS OR MORE
2	ICMP/Echo Reply PACKETS AT T2 Kbps OR MORE ARE CONTINUOUSLY TRANSMITTED FOR S2 SECONDS OR MORE
3	FRAGMENT PACKETS AT T3 Kbps OR MORE ARE CONTINUOUSLY TRANSMITTED FOR S3 SECONDS OR MORE
⋮	

## FIG.5

LEGITIMACY CONDITION TABLE

13c

NO.	DETECTION ATTRIBUTES
1	{Src=172.16.10.0/24}
2	{TOS=0x01}
⋮	

FIG.6

SIGNATURE LIST

16a

SIGNATURE TYPE	PRIORITY	PRIORITY ORDER	SIGNATURE
SET SIGNATURE [ <ul style="list-style-type: none"> <li>• ILLEGITIMATE SIGNATURE</li> <li>• LEGITIMATE SIGNATURE</li> <li>• SUSPECT SIGNATURE</li> </ul> ]	HIGHEST PRIORITY	1	SIGNATURE A
		2	SIGNATURE B
		:	
		X-1	
ILLEGITIMATE SIGNATURE	HIGH	X	SIGNATURE C
		X+1	
		:	
		Y-1	
LEGITIMATE SIGNATURE	MEDIUM	Y	SIGNATURE D
		Y+1	
		:	
		Z-1	
SUSPICIOUS SIGNATURE	LOW	Z	SIGNATURE E
		Z+1	SIGNATURE F
		:	

FIG.7

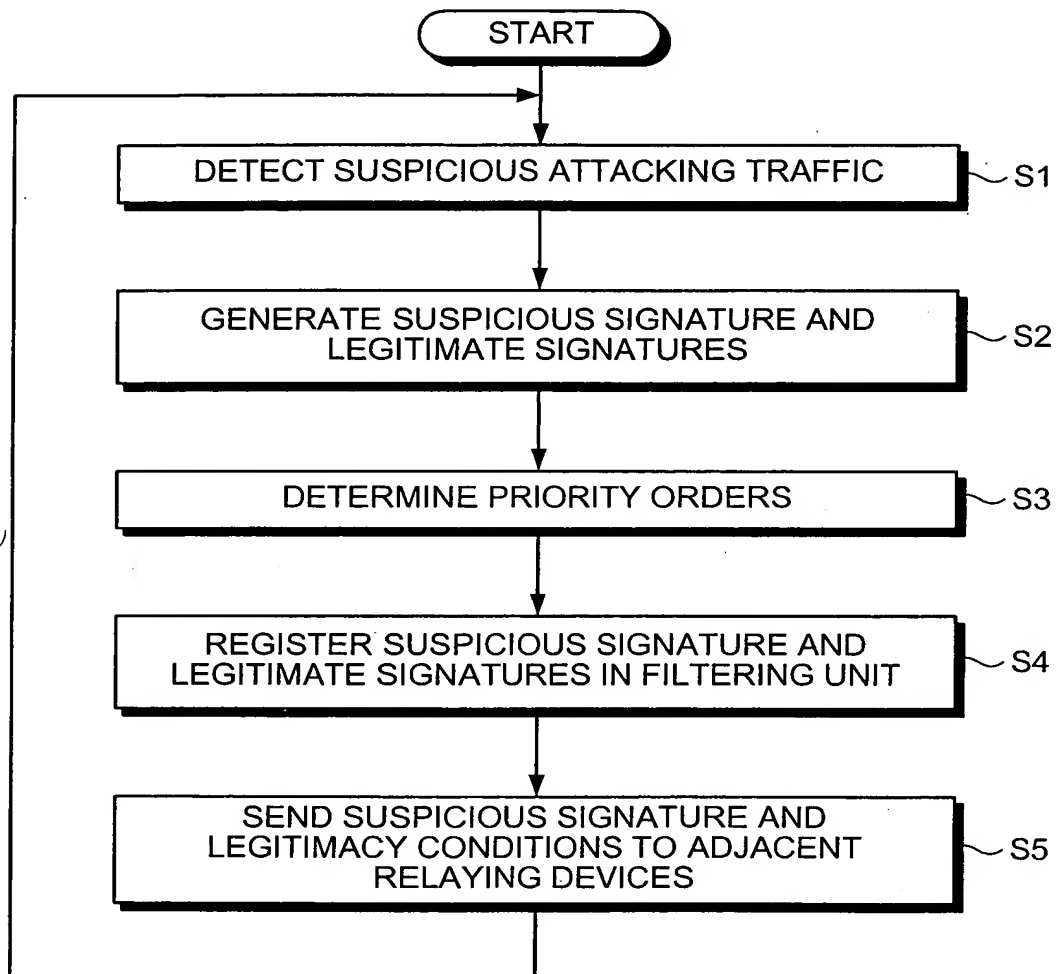


FIG.8

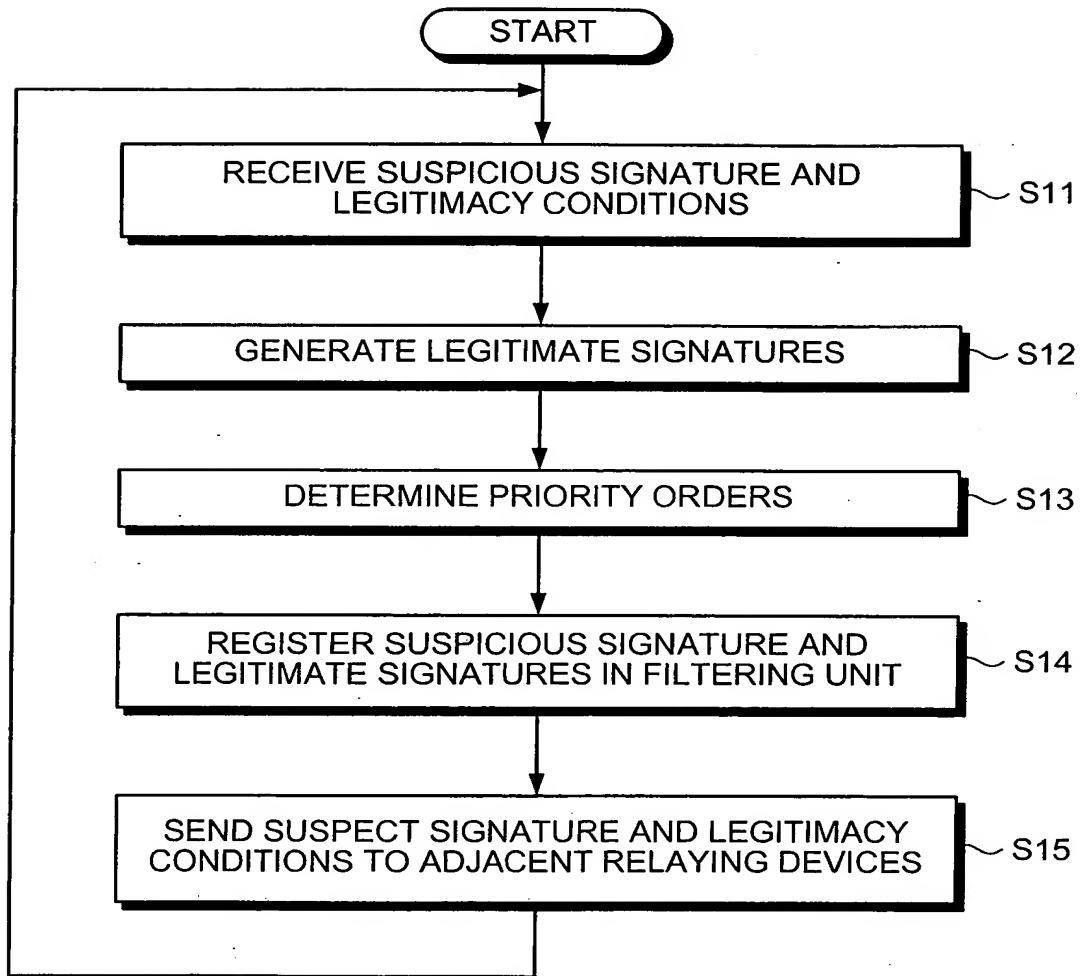


FIG.9

